Int. J. Adv. Res. Sci. Technol. Volume 15, Issue 3, 2026, pp. 2647-2655.

IJARST

International Journal of Advanced Research in Science and Technology

https://doi.org/10.62226/ijarst20262806

ISSN 2319 – 1783 (Print)
ISSN 2320 – 1126 (Online)

A Robust Optical Watermarking Scheme Using Phase Encoding in Gyrator Transform Domain

Nagander Singh Tomer[1*] and Anoop Kumar[2]

1*Assistant Professor of Mathematics, Department of Mathematics, Guru Gorakhnath Ji Govt. College, Hisar, Haryana, India,

2Assistant Professor of Mathematics, Department of Mathematics, Govt College Bahadurgarh Jhajjar, Haryana, India

Email *tomar.smart@gmail.com*

ARTICLEINFO

Article history:

Received	03 Sep 2026
Accepted	15 Sep 2026
Available online	25 Sep 2026

Keywords:

Optical watermarking; Image encryption; Phase encoding; Gyrator transform; Hessenberg decomposition; Umbrella chaotic map.

Indexed in:

and in major libraries

ABSTRACT

The increasing need for secure digital image protection has motivated the development of robust and imperceptible watermarking techniques. This work proposes an optical watermarking framework integrating phase encoding, random phase modulation, Gyrator transform, Hessenberg decomposition, and Umbrella-map-based chaotic scrambling for secure watermark embedding and extraction. The performance of the proposed scheme is evaluated using MSE, PSNR, SSIM, correlation coefficient, histogram analysis, pixel correlation, and noise robustness. The extracted watermark achieves an SSIM of 1 and a PSNR of 276.0824 dB, indicating excellent structural fidelity and negligible reconstruction distortion. Moreover, the watermark remains reliably recoverable under Gaussian noise with a strength of 1.5, demonstrating strong noise robustness. The results confirm that the proposed framework provides secure and high-quality watermarking with effective protection against noise, making it suitable for secure image communication, authentication, and copyright protection.

Introduction

The rapid growth of digital technologies has increased the use of digital images in healthcare, banking, remote sensing, defence, multimedia communication, and social networking. Since such images may contain sensitive or copyright-protected information, secure protection against unauthorized access, manipulation, and illegal distribution is essential. Consequently, image encryption and digital watermarking have become important techniques for secure communication, authentication, ownership verification, and copyright protection. An effective watermarking scheme should provide high imperceptibility, security, robustness, and reliable watermark recovery.

Optical image encryption has attracted considerable attention because optical systems offer inherent parallel processing capability, high computational speed, and multiple degrees of freedom for encoding information. One of the fundamental developments in this field was the double random phase encoding

(DRPE)[1] technique introduced by Refregier and Javidi in 1995. The conventional DRPE system employs a Fourier transform together with two statistically independent random phase masks to convert the plaintext image into an encrypted representation.Researchers have subsequently investigated different optical transforms to improve the flexibility and security of encryption systems. These include the fractional Fourier transform[2], [3], Fresnel transform[4], Hartley transform[5], [6], Gyrator transform[7], fractional Hartley transform[8], and [9], [10].

Among these transforms, the Gyrator transform (GT) is particularly attractive for optical information processing due to its rotational property and additional transform parameter. Its rotation angle provides an extra tunable parameter that can serve as a secret key, while enabling flexible control of spatial–frequency characteristics. These features make GT a promising tool for secure and flexible optical image encryption.

Although optical encryption techniques provide effective visual security, several investigations have demonstrated that conventional DRPE-based systems can be vulnerable to cryptanalytic attacks, including chosen-plaintext attack (CPA)[11], known-plaintext attack (KPA)[12], and ciphertext-only attack (COA)[13]. Such vulnerabilities arise primarily from the linear structure and symmetric nature of many

conventional optical encryption architectures. To overcome these limitations, asymmetric encryption strategies have also been explored. For example, Qin and Peng introduced an asymmetric optical encryption approach based on phase truncation[14]. Although asymmetric processing improved the security characteristics of optical encryption, subsequent studies reported vulnerabilities to iterative reconstruction and related attacks[15], [16]. These observations emphasize the necessity of developing encryption architectures with stronger key dependency, improved asymmetry, and enhanced resistance against different cryptanalytic attacks.

Phase encoding[17] has emerged as an effective technique for optical image encryption because it represents image information through a complex-valued phase distribution. In this approach, the intensity information of the original image is mapped into a phase representation, thereby concealing the direct visual appearance of the plaintext. Phase images can subsequently be combined with random phase modulation, optical transforms, chaotic systems, and matrix decomposition techniques to construct multilayer encryption architectures. Such combinations provide additional degrees of freedom for key generation and transformation, while also making unauthorized reconstruction considerably more difficult. Therefore, phase encoding can serve as an effective preprocessing stage for secure optical image processing.

In parallel with optical transforms, chaotic systems[18], [19] have become an important component of modern image encryption algorithms. Chaotic maps exhibit properties such as sensitivity to initial conditions, pseudo-random behaviour, ergodicity, and unpredictability, which make them suitable for generating sequences used in pixel permutation and diffusion. In the present work, the Umbrella map is employed to generate a chaotic sequence for scrambling and enhancing the security of the encrypted image.

Mathematical decomposition methods have also been increasingly incorporated into optical encryption frameworks. Techniques such as equal modulus decomposition[20], singular value decomposition[21], [22], unequal modulus decomposition[23], [24], [25], [26], [27], [28], random modulus decomposition[29], [30], and Hessenberg decomposition have been investigated for processing image information in different transform domains. In the proposed framework, Hessenberg decomposition is utilized to introduce an asymmetric processing structure and to strengthen the overall security of the encryption architecture.

In addition to encryption, secure image watermarking[31], [32], [33], [34], [35] has become increasingly important for protecting intellectual property and ensuring the authenticity and integrity of digital content. Watermarking provides information for ownership, authentication, copyright, and content verification, but must balance imperceptibility, robustness, capacity, and security. Unprotected watermark embedding may allow unauthorized extraction, modification, or removal. Integrating watermarking with optical encryption, chaotic scrambling, and matrix decomposition can enhance security while preserving the quality and robustness of the recovered image and watermark, enabling secure image communication and authentication.

Motivated by these considerations, this paper proposes a secure optical image encryption and watermarking framework based on the Gyrator transform, Hessenberg decomposition, phase encoding, and Umbrella-map-based chaotic scrambling. The Gyrator transform introduces an additional transform parameter, while Hessenberg decomposition contributes an asymmetric processing stage. The Umbrella chaotic map is employed to generate pseudo-random sequences for image scrambling, thereby improving the confusion characteristics of the cryptosystem. The watermarking component further enables secure embedding and recovery of additional information for applications such as copyright protection, authentication, and secure image communication. The performance of the proposed method is evaluated using reconstruction quality, statistical characteristics, key sensitivity, differential attack analysis, and robustness tests involving noise and occlusion. The results demonstrate the potential of the proposed framework for secure transmission and protection of digital images.

The remainder of this paper is organized as follows. Section 2 presents the theoretical foundations of the proposed framework. Section 3 describes the watermark embedding and extraction procedures. Section 4 presents the experimental and security analyses. Finally, Section 5 concludes the paper.

2. Basic terminology

In this section, we discuss the mathematical transforms and decomposition in detail.

2.1 Gyrator transform

The Gyrator Transform (GT) is a linear canonical integral transform that extends the Fourier transform by introducing a rotation parameter. It provides a continuous transition between spatial and frequency domains. For a 2-D function $f(x,y)$, the GT is defined mathematically as

$$G_\alpha(u,v) = \iint f(x,y)K_\alpha(x,y,u,v)dxdy \quad (1)$$

where, kernel is defined as:

$$K_\alpha(x,y,u,v) = \frac{1}{|sin\alpha|}\exp\left[i2\pi\frac{(ux+vy)cos\alpha-(uv+xy)}{sin\alpha}\right] \quad (2)$$

Its rotation parameter determines the transformation characteristics. For $\alpha = 0$, no rotation occurs and the GT reduces to the identity operation. At $\alpha = \pm\frac{\pi}{2}$, it becomes equivalent to the Fourier transform and inverse Fourier transform. Since the transformation represents a rotation, it is periodic with period 2π, i.e., a rotation by2π restores the original representation.

2.2 Hessenberg Decomposition

Hessenberg Decomposition (HD) is a matrix factorization method that transforms a square matrix into a Hessenberg matrix through a similarity

transformation involving a unitary matrix. This decomposition is widely used in numerical linear algebra because it simplifies matrix operations while preserving the eigenvalues of the original matrix. The decomposition of a square matrix A can be expressed as

$$A = PHP^{*} \quad (3)$$

Here, A is any square matrix, P is unitary matrix i.e. $PP^{*} = P^{*}P = I$ and H is Hessenberg matrix i.e. H is a matrix in which all entries below the first sub-diagonal are zero.

2.3 Umbrella Map

The Tinkerbell map is a two-dimensional nonlinear discrete chaotic system defined:

$$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n \quad (4)$$

$$y_{n+1} = 2x_n y_n + cx_n + dy_n \quad (5)$$

where denotes the iteration number, and are the state variables, and are system parameters.

A modified form of the Tinkerbell map, known as the Umbrella map, is obtained by incorporating the sine function into the nonlinear terms. It is expressed as

$$x_{n+1} = \sin(x_n^2) - y_n^2 + \text{asin}(x_n) + by_n \quad (6)$$

$$y_{n+1} = \sin(2x_n)y_n + c\sin(x_n) + dy_n \quad (7)$$

Here, n-represents the iteration index, while a, b, c, d are the control parameters. In this study, the parameter values are selected as a=0.874, b$\epsilon(-0.6013, 0.5142)$, c=2, and d=0.5, with initial conditions $x_0 = 0.1787$ and $y_0 = 0.178$. These values are used for the numerical generation of the chaotic sequence.

3 Proposed Watermarking Scheme

The proposed watermarking framework is designed to provide secure embedding and reliable extraction of a phase-encoded image.

3.1 Watermarking Embedding

Step 1 Let I_p denote the input grayscaleimage of size 256×256. The normalized image is converted into a phase-only representation and stored as I

$$I = \exp[i2\pi I_p] \quad (8)$$

Step 2 The phase image is multiplied with RPM1 to introduce an additional random phase component the output is stored as I_1

$$I_1 = I \times \text{RPM1} \quad (9)$$

Step 3 The modulated phase image is then subjected to a Gyrator Transform (GT) with an appropriate rotation parameter α and the output is stored asI_2

$$I_2 = \text{GT}(I_1, \alpha_1) \quad (10)$$

Step 4 I_2pixels are scrambled using Umbrella map, and the result is stored as H_2 which is mathematically given as:

$$I_3 = Scrambling(I_2, \text{Umbrella } map) \quad (11)$$

Step5 The scrambled transform-domain matrix is then subjected to Hessenberg decomposition.

$$[\text{key1}, H] = HD(I_3) \quad (12)$$

Here key1 is stored as private key which is used in extraction process.

Step 6 The resulting encrypted representation is further multiplied by a second independently generated random phase mask RPM2 and output is stored as I_4

$$I_4 = H \times \text{RPM2} \quad (13)$$

Step 7 After the second random phase modulation, the resulting data is processed through another Gyrator transform and output is stored as I_5

$$I_5 = \text{GT}(I_4, \alpha_2) \quad (14)$$

$$\text{key2} = angle(I_5) \quad (15)$$

$$I_6 = abs(I_5) \quad (16)$$

Step 8 The encrypted image is embedded into the host image K with an attenuation factor a to obtain the watermarked image I_6, which is mathematically represented as:

$$I_7 = \text{K} + a \times I_6 \quad (17)$$

The complete watermarking process's flow chart is shown in Fig. 1.

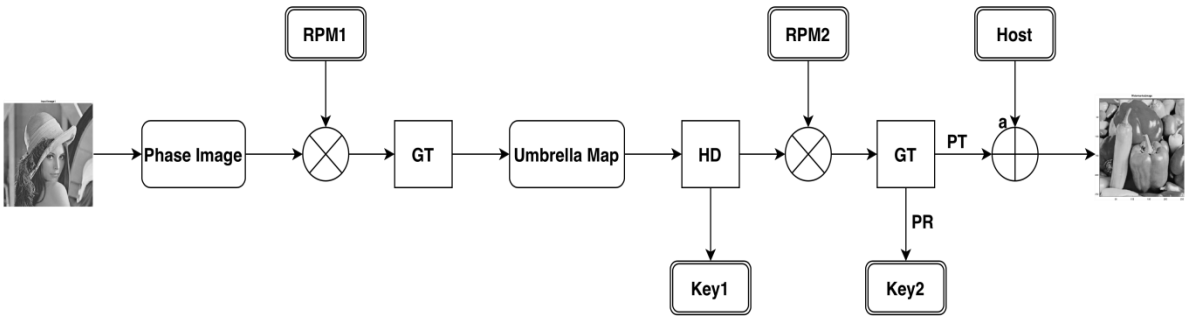

Fig. 1 Schematic flow chart of watermarking algorithm.

3.2 Watermarking Extraction Process

The watermark extraction process is comparatively straightforward and primarily involves the inverse operations of the embedding procedure.

Step 1 Initiallythe host image K is subtracted from the watermarked image I_7 and divided by the attenuation factor a to obtain the encrypted watermark I_6. It is then multiplied by key2 to obtain I_5, the output is stored as D_1given by:

$$D_1 = \frac{I_7 - \text{K}}{a} \times \text{key2} \quad (18)$$

Step 2 D_1undergoes the inverse Gyrator transform (IGT) with angle $-\alpha_2$, followed by multiplication with $Conj(\text{RPM2})$, output is stored as D_2

$$D_2 = \text{IGT}[D_1, -\alpha_2] \times Conj(\text{RPM2}) \quad (19)$$

Step 3 D_2 is subjected to the inverse Hessenberg decomposition using key1, output is stored as D_3

$$D_3 = \text{key1} \times D_2 \times \text{key1}' \quad (20)$$

Step 4 The pixels of D_3 are descrambled using the inverse Umbrella map to obtain D_4:

$$D_4 = \text{Descramble}(\text{D}_3, \text{Umbrella map}) \quad (21)$$

Step 5 $D_4$is subjected to the inverse Gyrator transform with angle $-\alpha_1$ and multiplied by $Conj(\text{RPM1})$ to recover the phase image output is stored as D_5

$$D_5 = \text{IGT}[D_4, -\alpha_1] \times Conj(\text{RPM1}) \quad (22)$$

Finally we get D_5 as our extracted image. The flow chart is given in Fig. 2.

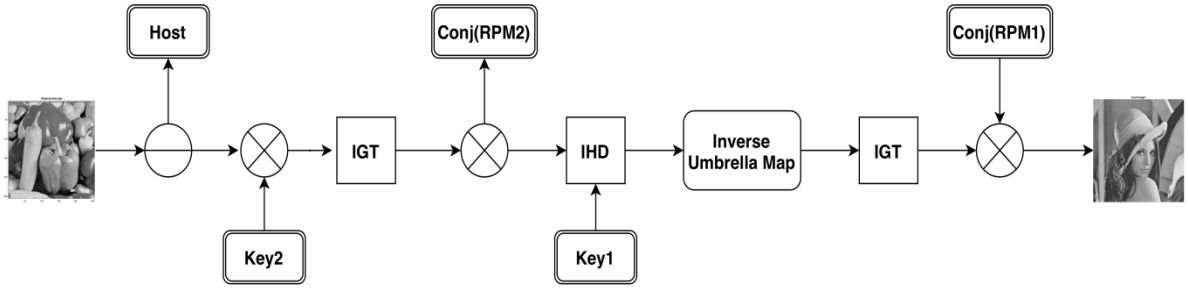

Fig. 2 Schematic flow chart of extracting algorithm

.

4 Experimental Validation

The proposed encryption scheme was implemented and tested in MATLAB R2025b on a computer featuring an Intel Core i7 processor and 32 GB of RAM. The experimental results are presented and analysed in detail to demonstrate the effectiveness, robustness, and security of the proposed encryption framework.

4.1 Visual Analysis

To assess the security, robustness, and computational efficiency of the proposed cryptosystem, extensive simulations were performed using grayscale images of varying dimensions. For illustration, the results obtained for the Lena image with a size of 256 × 256 pixels are presented in this section. The original, watermarked, and decrypted images are shown in Fig. 3. It can be observed that the watermarked image preserves the visual appearance of the host image while embedding the encrypted information with minimal perceptual distortion. The embedded information remains imperceptible under normal visual inspection, indicating the effectiveness of the proposed watermarking scheme.

Fig. 3 Visual results corresponding to (a) Input image, (b) Watermarked image, and (c) Extracted image.

In contrast, the decrypted image closely resembles the original input image, demonstrating the accurate recovery capability of the proposed approach. These results confirm that the proposed scheme effectively conceals the embedded information while maintaining the visual quality of the watermarked image and enabling reliable information recovery. Computational Complexity for the proposed process requires approximately 1.522 s for watermarking and 1.779 s for the complete watermarking and extraction process.

4.2 Correlation Coefficient

The Correlation Coefficient (CC) is used to measure the similarity between two images. It is defined as

$$CC = \frac{cov(I', DI_5)}{\sigma_{I'}\sigma_{DI_5}} \quad (23)$$

where, I'denote input image and DI_5 denote decrypted image. The term $cov(IP, DI)$ represents the covariance between input and decrypted images, while σ_{IP}, σ_{DI} correspond to the standard deviations of the input and decrypted images. A CC value close to 1 indicates high similarity, whereas a value close to 0 indicates negligible correlation.

For the proposed scheme, the CC between the input and decrypted images is 1, demonstrating accurate image reconstruction. In contrast, the CC between the input and encrypted images is 0.0031, which is very close to zero and indicates that the encryption process effectively removes the statistical correlation of the

original image. For watermarking, a high CC between the original and extracted watermark indicates successful and reliable watermark recovery.

4.3 Mean Squared Error (MSE)

The mean squared error (MSE) is a commonly used quantitative measure for assessing the reconstruction quality of an image. It represents the average squared difference between the corresponding pixel intensities of the original input image and the decrypted image. The MSE can be expressed as

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{M-1} \sum_{j=0}^{N-1} [I'(i,j) - DI_5(i,j)]^2 \quad (24)$$

$I'(i,j)$ and $DI_5(i,j)$ denotes the pixel values at position (i,j) in the input and decrypted images respectively.While, M and N represent the dimensions of the image. A smaller MSE value indicates a lower reconstruction error and, consequently, greater similarity between the input and decrypted images. In the proposed method, the obtained MSE value is2.4647×10^{-28}, which is very close to zero. This indicates that the decrypted image closely reproduces the original image, thereby confirming the high reconstruction accuracy of the proposed encryption framework.

4.4 Peak Signal to Noise Ratio (PSNR)

The Peak Signal-to-Noise Ratio (PSNR) is a widely used objective measure for evaluating the quality of a reconstructed or recovered image with respect to its original counterpart. It quantifies the level of distortion introduced during the processing by relating the maximum possible pixel intensity to the mean squared error (MSE) between the original and extracted images. A higher PSNR value generally indicates lower reconstruction error and, consequently, better image fidelity.The PSNR can be expressed as

$$PSNR = 10log_{10}\left(\frac{max^2}{MSE}\right) \quad (25)$$

where max denotes the maximum possible intensity value of a pixel, while MSE represents the mean squared error between the original and extracted images. For an 8-bit grayscale image, the maximum pixel intensity is 255.

The PSNR obtained for the proposed algorithm is 276.0824dB. The relatively high PSNR value demonstrates that the reconstructed image maintains a high degree of similarity with the original image, with only a negligible amount of distortion.

Therefore, the obtained PSNR result confirms the effectiveness of the proposed scheme in achieving high-quality image reconstruction.A comparative analysis of PSNR and MSE of our proposed scheme with some other articles is given in Table 1.

Metrices	R. Yadav and P. Singh[35]	Archana et al.[36]	Qingtang Su et al.[37]	Proposed Scheme
PSNR	_	82.7337 dB	42.8764 dB	276.0824 dB
MSE	1.025×10^{4}	8.1213×10^{-13}	-	2.4647×10^{-28}

Table 1. Comparative analysis of PSNR and MSE.

4.5 Structural Similarity Index Metric

The Structural Similarity Index Measure (SSIM) is a widely adopted full-reference metric for evaluating the perceptual quality of an extracted image with respect to its corresponding original image. In the proposed watermarking framework, SSIM is used to quantify how effectively the embedded watermark information is recovered during the extraction process. Unlike conventional error-based measures, SSIM evaluates image similarity by considering three important components: luminance, contrast, and structural information. Its value generally ranges from −1 to 1, where a value closer to 1 indicates a higher degree of structural similarity. The SSIM between the original I' and the extracted watermark DI_5 is defined as

$$SSIM(I,D) = \frac{(2\mu_{I'}\mu_{DI_5}+C_1)(2cov(I',DI_5)+C_2)}{(\mu_{I'}^2+\mu_{DI_5}^2+C_1)(\sigma_{I'}^2+\sigma_{DI_5}^2+C_2)} \quad (26)$$

where $\mu_{I'}$ and μ_{DI_5} represent the mean intensities of the original and extracted watermark images, respectively. The quantities $\sigma_{I'}^2$ and $\sigma_{DI_5}^2$ denote their respective variances, whereas $cov(I', DI_5)$ represents the covariance between the original and extracted watermarks. The constants C_1 and C_2 are small positive values introduced to ensure numerical stability and avoid division by zero.

For the proposed watermarking scheme, an SSIM value of 1 is obtained between the original and extracted watermark images. The value being very close to unity indicates that the extracted watermark retains almost all the structural characteristics of the original watermark. This result demonstrates the high fidelity and accuracy of the watermark extraction process, confirming that the proposed scheme can recover the embedded information with negligible structural distortion.

4.6 Statistical Attack Analysis Histogram and 3D Plots

Histogram analysis is an important statistical tool for evaluating the security and visual characteristics of image encryption and watermarking schemes. It represents the frequency distribution of pixel intensity

levels and can be used to examine the extent to which the statistical properties of an image are altered during the processing stages.

As shown in Fig. 4, the histogram of the watermarked image exhibits a distribution that differs considerably from that of the original image. This alteration in the intensity distribution indicates that the watermark embedding and associated encryption operations effectively modify the statistical characteristics of the host image, thereby reducing the possibility of direct statistical analysis. At the same time, the watermarked image maintains its visual content with only limited perceptual distortion.

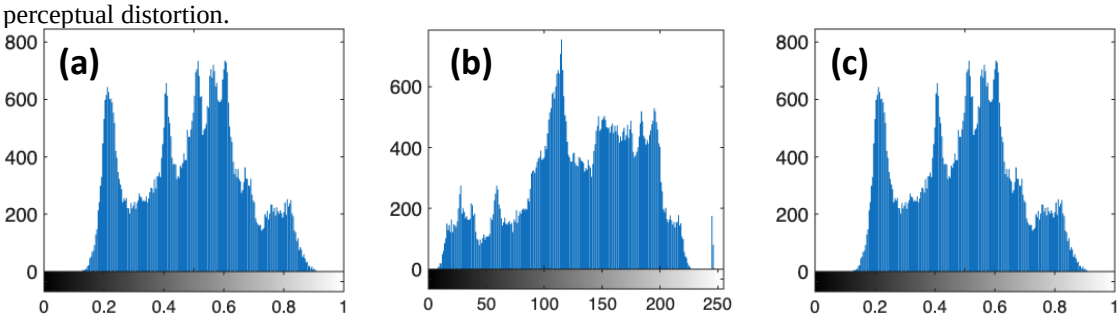

Fig. 4 Histogram of (a) Input image, (b) Watermarked image, and (c) Extracted image.

Three-dimensional (3D) surface plots provide a visual representation of the spatial distribution of pixel intensities and are useful for examining variations in image structure. In the proposed watermarking framework, 3-D surface analysis is employed to investigate the changes introduced during the watermark embedding and extraction processes and to assess the preservation of the host image characteristics.

As depicted in Fig. 5, the 3-D surface corresponding to the original image exhibits a relatively smooth and coherent profile, reflecting the spatial continuity and inherent correlations of the image content. After watermark embedding, the surface profile of the watermarked image shows noticeable variations

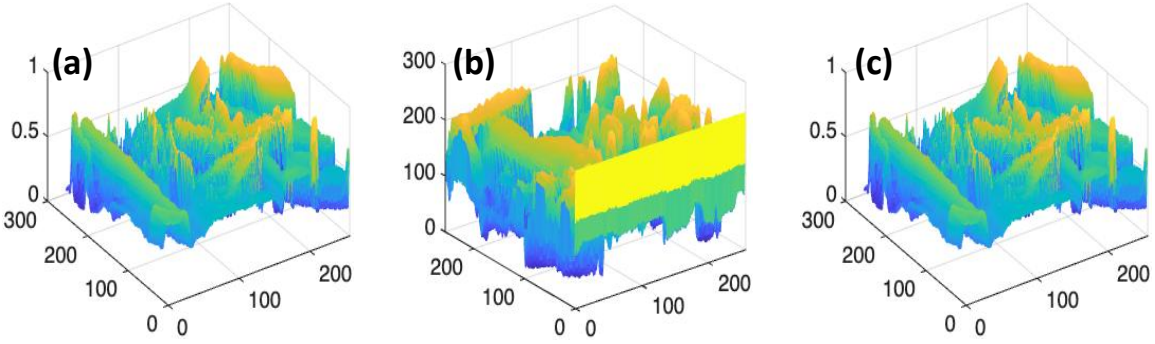

Fig. 5 Three-dimensional surface representations of (a) Input image, (b) Watermarked image, and (c) Extracted image.

Furthermore, the histogram of the extracted watermark closely follows the distribution of the original watermark, demonstrating the accurate recovery of the embedded information. The high similarity between the original and extracted watermark histograms confirms that the proposed scheme preserves the essential statistical characteristics of the watermark during the embedding and extraction processes. Overall, these results demonstrate the effectiveness of the proposed watermarking framework in providing secure information embedding, statistical concealment, and reliable watermark extraction compared with the original image. These changes indicate the modifications introduced by the embedding operation while retaining the overall spatial characteristics of the host image. The absence of excessive surface distortion further suggests that the watermark is embedded without causing significant degradation to the host image.

Furthermore, the 3-D surface plot of the extracted watermark closely follows the spatial profile of the original image, demonstrating the effectiveness of the proposed extraction mechanism. The structural correspondence between the original and extracted watermark surfaces confirms that the embedded information can be recovered with high fidelity. Therefore, the 3-D surface analysis provides qualitative evidence of the imperceptibility of watermark embedding and the reliable recovery of the embedded information, supporting the overall effectiveness of the proposed watermarking scheme.

4.7 Noise Attack Analysis

During practical transmission and storage, the watermarked image may be affected by channel or environmental noise, which can degrade the quality of the extracted watermark. Therefore, the robustness of a watermarking scheme should be evaluated under different noise conditions to determine its ability to

preserve the embedded information. In this study, additive Gaussian noise is introduced into the watermarked image to simulate a noisy transmission channel. The noisy watermarked image can be represented as

$$noisy\ image = ciphertext + \sigma \times \mathrm{N} \quad (27)$$

where σ denotes the noise strength, and Nis a Gaussian random variable with zero mean and unit variance.

To investigate the noise resilience of the proposed watermarking scheme, the watermarked image was subjected to different levels of Gaussian noise, followed by the watermark extraction process. The extracted watermark was then compared with the original watermark using appropriate quality measures. The experimental results demonstrate that the embedded watermark remains recognizable even as the noise intensity increases.

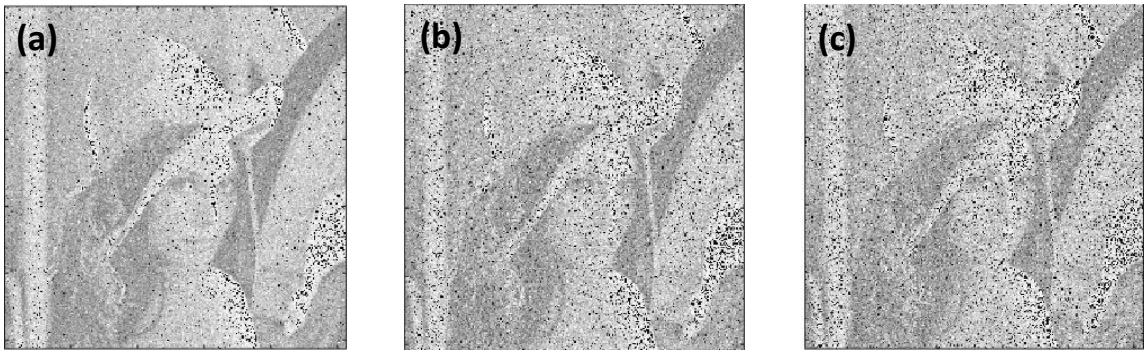

Fig. 6 Watermark extraction results under varying levels of additive Gaussian noise when noise strength (a) $\sigma = 0.5$, (b) $\sigma = 1$, and (c) $\sigma = 1.5$

In particular, the proposed scheme maintains satisfactory extraction performance at a noise strength of 1.5, indicating its ability to tolerate a considerable level of additive noise. This behaviour demonstrates the robustness of the proposed watermarking framework against noise-induced distortions and confirms its suitability for reliable watermark transmission over imperfect communication channels.

4.8 Correlation Distribution Analysis

Pixel correlation analysis is performed to evaluate the extent to which the proposed encryption scheme disrupts the spatial dependency between neighbouring pixels. For this purpose, 5000 pairs of adjacent pixels are randomly selected along the diagonal direction from the input and encrypted images, as illustrated in Fig. 7. The input image exhibits a distinct linear pattern, indicating a strong correlation among neighbouring pixels, which is a characteristic feature of natural images. In contrast, the encrypted image shows a widely scattered and irregular distribution of pixel pairs, demonstrating a substantial reduction in spatial correlation. The pronounced difference between the pixel distributions of the input and encrypted images indicates that the proposed scheme effectively obscures the inherent spatial relationships and statistical characteristics of the original image. This behaviour enhances the confidentiality of the embedded information and reduces the possibility of exploiting pixel dependencies through statistical or correlation-based attacks.

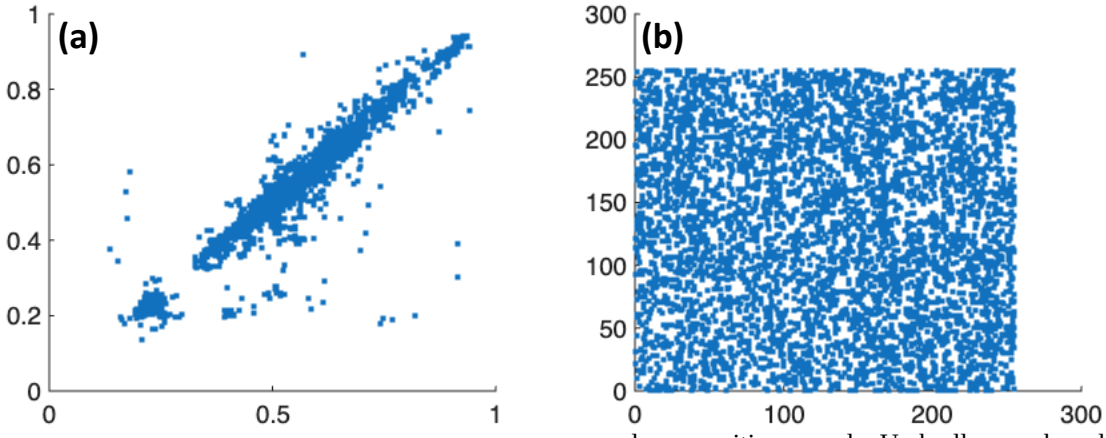

Fig. 7 Correlation distribution plot (a) Input images, (b)Encrypted image.

5 Conclusion

In this work, a secure and robust optical watermarking framework based on phase encoding, random phase modulation, Gyrator transform, Hessenberg decomposition, and Umbrella-map-based chaotic scrambling has been presented. The proposed approach effectively embeds phase-encoded information into a host image while preserving its visual quality and enabling reliable watermark extraction. The experimental results demonstrate excellent reconstruction fidelity, with an SSIM of 1

and a PSNR of 276.0824dB, confirming the high structural similarity and negligible distortion of the extracted watermark. Statistical and structural analyses further validate the effectiveness of the proposed framework. In addition, the scheme exhibits satisfactory resilience against additive Gaussian noise, with reliable watermark recovery maintained at a noise strength of 1.5. Overall, the obtained results establish that the proposed watermarking framework offers a favourable combination ofimperceptibility, extraction accuracy, and robustness, making it a promising solution for applications involving image authentication, copyright protection, and secure multimedia communication.

References

[1] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Optics Letters*, vol. 20, pp. 767–769, 1995, doi: 10.1364/OL.20.000767.

[2] N. K. Nishchal, J. Joseph, and K. Singh, "Fully phase encryption using fractional Fourier transform," *Optical Engineering*, vol. 42, no. 6, pp. 1583–1588, Jun. 2003, doi: 10.1117/1.1570429.

[3] S. Anjana, I. Saini, P. Singh, and A. K. Yadav, "Asymmetric enciphering of images using affine transform and fractional Fourier transform," *Int. J. Advanced Intelligence Paradigms*, vol. 29, no. 1, pp. 28–45, Sep. 2024, doi: 10.1504/IJAIP.2024.141523.

[4] Shalu, A. K. Yadav, and P. Singh, "Nonlinear multiple color image encryption using Quasinormal-Zernike Algorithm in Fresnel transform domain," *J Opt*, Oct. 2025, doi: 10.1007/s12596-025-02940-z.

[5] A. K. Yadav, P. Singh, I. Saini, and K. Singh, "Asymmetric encryption algorithm for colour images based on fractional Hartley transform," *Journal of Modern Optics*, vol. 66, pp. 629–642, 2019, doi: 10.1080/09500340.2018.1559951.

[6] P. Singh, A. K. Yadav, S. Vashisth, and K. Singh, "Review of optical image encryption schemes based on fractional Hartley transform," *Asian Journal of Physics*, vol. 28, no. 7–9, pp. 701–716, 2019, doi: 10.1063/1.4973267.

[7] J. A. Rodrigo, T. Alieva, and M. L. Calvo, "Applications of gyrator transform for image processing," *Optics Communications*, vol. 278, pp. 279–284, 2007, doi: 10.1016/j.optcom.2007.06.023.

[8] A. K. Yadav, P. Singh, I. Saini, and K. Singh, "Asymmetric encryption algorithm for colour images based on fractional Hartley transform," *Journal of Modern Optics*, vol. 66, no. 6, pp. 629–642, Mar. 2019, doi: 10.1080/09500340.2018.1559951.

[9] Shalu, A. K. Yadav, and P. Singh, "Uniquely designed optical cryptosystem for watermarking of double-color images in the fractional Hermite-transform domain," *Opt. Eng.*, vol. 64, no. 09, Sep. 2025, doi: 10.1117/1.OE.64.9.093101.

[10] Shalu, P. Singh, and A. K. Yadav, "Watermarking based on asymmetric dual-image encryption using QZ algorithm and vortex toroidal lenses in fractional Hermite transform domain," *Optik*, vol. 342–343, p. 172598, Dec. 2025, doi: 10.1016/j.ijleo.2025.172598.

[11] X. Peng, H. Wei, and P. Zhang, "Chosen-plaintext attack on lensless double-random phase encoding in the Fresnel domain," *Optics letters*, vol. 31, no. 22, pp. 3261–3263, Nov. 2006, doi: 10.1364/OL.31.003261.

[12] X. Peng, P. Zhang, H. Wei, and B. Yu, "Known-plaintext attack on optical encryption based on double random phase keys," *Optics Letters*, vol. 31, pp. 1044–1046, 2006, doi: 10.1364/OL.31.001044.

[13] G. Li, W. Yang, D. Li, and G. Situ, "Ciphertext-only attack on the double random-phase encryption: Experimental demonstration," *Optics Express*, vol. 25, no. 8, pp. 8690–8697, Apr. 2017, doi: 10.1364/OE.25.008690.

[14] W. Qin and X. Peng, "Asymmetric cryptosystem based on phase-truncated Fourier transforms," *Opt. Lett.*, vol. 35, no. 2, p. 118, Jan. 2010, doi: 10.1364/OL.35.000118.

[15] X. Wang, Y. Chen, C. Dai, and D. Zhao, "Discussion and a new attack of the optical asymmetric cryptosystem based on phase-truncated Fourier transform," *Appl. Opt.*, vol. 53, no. 2, p. 208, Jan. 2014, doi: 10.1364/AO.53.000208.

[16] Y. Wang, C. Quan, and C. J. Tay, "New method of attack and security enhancement on an asymmetric cryptosystem based on equal modulus decomposition," *Appl. Opt.*, vol. 55, no. 4, p. 679, Feb. 2016, doi: 10.1364/AO.55.000679.

[17] X. Deng and W. Wen, "Optical multiple-image encryption based on fully phase encoding and interference," *Optik*, vol. 126, no. 21, pp. 3210–3214, Nov. 2015, doi: 10.1016/j.ijleo.2015.07.148.

[18] Sachin and P. Singh, "A novel chaotic Umbrella map and its application to image encryption," *Opt Quant Electron*, vol. 54, no. 5, p. 266, May 2022, doi: 10.1007/s11082-022-03646-3.

[19] Sachin and P. Singh, "Analysis of chaotic patterns in the Bird wing map and implications in image security," *Journal of Modern Optics*, vol. 72, pp. 603–628, May 2025, doi: 10.1080/09500340.2025.2508790.

[20] J. Cai and X. Shen, "Modified optical asymmetric image cryptosystem based on coherent superposition and equal modulus decomposition," *Optics & Laser Technology*, vol. 95, pp. 105–112, Oct. 2017, doi: 10.1016/j.optlastec.2017.04.018.

[21] H. Singh, K. S. Gaur, S. Thakran, and K. Singh, "An asymmetric phase image encryption technique using Arnold transform, singular

value decomposition, Hessenberg decomposition, and fractional Hartley transform," Appl. Phys. B, vol. 130, no. 10, p. 186, Oct. 2024, doi: 10.1007/s00340-024-08312-y.

[22] P. Singh, A. K. Yadav, and K. Singh, "Phase image encryption in the fractional Hartley domain using Arnold transform and singular value decomposition," *Optics and Lasers in Engineering*, vol. 91, pp. 187–195, Apr. 2017, doi: 10.1016/j.optlaseng.2016.11.022.

[23] Archana, Sachin, and P. Singh, "Cascaded unequal modulus decomposition in Fresnel domain based cryptosystem to enhance the image security," *Optics and Lasers in Engineering*, vol. 137, pp. 106399–106411, Feb. 2021, doi: 10.1016/j.optlaseng.2020.106399.

[24] Archana, P. Singh, and P. Rakheja, "Asymmetric watermarking scheme for color images using cascaded unequal modulus decomposition in Fourier domain," *Journal of Modern Optics*, vol. 68, no. 20, pp. 1094–1107, Nov. 2021, doi: 10.1080/09500340.2021.1977404.

[25] S. Sachin, R. Kumar, and P. Singh, "Unequal modulus decomposition and modified Gerchberg Saxton algorithm based asymmetric cryptosystem in Chirp-Z transform domain," *Opt Quant Electron*, vol. 53, no. 5, pp. 254–274, May 2021, doi: 10.1007/s11082-021-02908-w.

[26] Sachin, P. Singh, R. Kumar, and A. K. Yadav, "Asymmetric cryptosystem for color images based on unequal modulus decomposition in Chirp-z domain," in *Proceedings of Academia-Industry Consortium for Data Science*, G. Gupta, L. Wang, A. Yadav, P. Rana, and Z. Wang, Eds., in Advances in Intelligent Systems and Computing, vol. 1411. Singapore: Springer Nature, 2022, pp. 331–344. doi: 10.1007/978-981-16-6887-6_27.

[27] I. Saini and N. Sharma, "Asymmetric multi-image wavelength multiplexing cryptosystem using QZ algorithm and unequal modulus decomposition," *Optics & Laser Technology*, vol. 172, p. 110505, May 2024, doi: 10.1016/j.optlastec.2023.110505.

[28] R. Yadav, S. Sachin, Archana, P. Singh, and A. K. Yadav, "Image encryption algorithm for color images based on cascaded unequal modulus decomposition in Fourier domain," *Asian Journal of Physics*, vol. 30, no. 7, pp. 1071–1082, Jul. 2021.

[29] S. Anjana, A. Yadav, P. Singh, and H. Singh, "Audio and image encryption scheme based on QR decomposition and random modulus decomposition in Fresnel domain," *OpticaApplicata*, vol. 52, no. 3, pp. 359–374, 2022, doi: 10.37190/oa220303.

[30] R. Yadav and P. Singh, "Asymmetric image authentication algorithm using double random modulus decomposition and CGI," *Computational and Applied Mathematics*, vol. 42, no. 7, p. 305, Sep. 2023, doi: 10.1007/s40314-023-02443-2.

[31] A. Archana, P. Singh, and P. Rakheja, "Asymmetric watermarking scheme for color images using cascaded unequal modulus decomposition in Fourier domain: Journal of Modern Optics: Vol 68, No 20." Accessed: Dec. 03, 2022. [Online]. Available: https://www.tandfonline.com/doi/abs/10.1080/09500340.2021.1977404.

[32] I. Mehra and N. K. Nishchal, "Optical asymmetric watermarking using modified wavelet fusion and diffractive imaging," *Optics and Lasers in Engineering*, vol. 68, pp. 74–82, May 2015, doi: 10.1016/j.optlaseng.2014.12.006.

[33] P. Singh, A. K. Yadav, K. Singh, and I. Saini, "Asymmetric watermarking scheme in fractional Hartley domain using modified equal modulus decomposition," *Journal of Optoelectronics and Advanced Materials*, vol. 21, no. 7–8, pp. 484–491, 2019.

[34] A. K. Yadav, S. Vashisth, H. Singh, and K. Singh, "A phase-image watermarking scheme in gyrator domain using devil's vortex Fresnel lens as a phase mask," *Optics Communications*, vol. 344, pp. 172–180, 2015.

[35] R. Yadav, Sachin, and P. Singh, "Watermarking algorithm based on phase-only CGH in fractional Hartley domain for DICOM images," *J. Opt.*, vol. 26, no. 6, p. 065703, May 2024, doi: 10.1088/2040-8986/ad3a77.

[36] Archana, P. Singh, and P. Rakheja, "Asymmetric watermarking scheme for color images using cascaded unequal modulus decomposition in Fourier domain," *Journal of Modern Optics*, vol. 68, no. 20, pp. 1094–1107, Nov. 2021, doi: 10.1080/09500340.2021.1977404.

[37] Q. Su, S. Chen, H. Wang, H. Cao, and F. Hu, "An efficient watermarking scheme for dual color image with high security in 5G environment," *Expert Systems with Applications*, vol. 249, p. 123818, Sep. 2024, doi: 10.1016/j.eswa.2024.123818.